Marko Jung

Galactic Viceroy of Research Excellence

m@mju.ng @mjung fb.com/markohjung

Information Security

Information Security

Information Security

it depends...

Organisations see the game as chess, laying out their own assets in a strategic manner trying to outthink the adversary.

Attackers are playing poker, trying to bluff and gamble their way in.


Play both
games!

CSIRTs, CIRTs, CERTs, SIRTs, or IRTs

A **Computer Security Incident Response Team** (with any of the above acronyms) is a concrete organisational entity that is assigned the **responsibility for coordinating and supporting the response to a computer security event or incident**.

The goal of a CSIRT is to minimise and control the damage resulting from incidents, provide effective guidance for response and recovery activities, and work to prevent future incidents from happening.

Source: https://www.us-cert.gov/

Key Requirements

Along with an **effective incident response handbook** (playbook), and a **mandate to protect the organisation**, great teams will also possess:

- **Adequate resources, tooling, and training** availabilities for the team to remain relevant and effective.
- Proper documentation and **understanding of what must be protected**.
- Documented and **reliable relationships** with other groups in the organisation.

OxCERT

University of Oxford Computer Emergency Response Team

1994 Founded as a group of volunteers across Oxford

1998 FIRST membership

2001 Full time staff as part of central Networks Team

2013 Information Security Team

2017 Five full time staff

The Four Core Questions

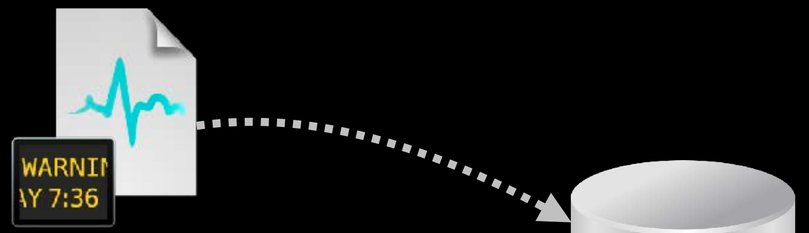
The core foundation to security monitoring and incident response:

1. What are we trying to protect?
2. What are the threats?
3. How do we detect them?
4. How do we respond?

Understanding that there will always be a place for incident prevention, while also recognizing that not every threat can be blocked, ensures a pragmatic approach to detection and response.

The Tool Maketh the Team

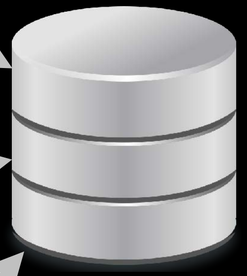
UNIVERSITY OF OXFORD



Logs & Events

Traffic analysis

Compliance



SIEM

Data aggregation
Correlation
Alerting
Retention
Forensic analysis
Reporting

Logs & Event Ingest

UNIVERSITY OF OXFORD

beats

Collection of lightweight data shippers for Elasticsearch

Filebeat, Winlogbeat, Heartbeat, Metricbeat, Packetbeat

logstash

Data processing pipeline with a variety of input formats

e.g. syslog, log4j, puppet facter, rss, https, rss, snmptrap

- Variety of filter plug-ins
- Powerful post-processing
- Data aggregation and pruning

NetFlow – Traffic Metadata

NetFlow also known as Jflow, Netstream, Cflowd, sflow, and IPFIX vary slightly, but the essence is the same: each technology creates a record of connections (a flow) between at least two hosts, including metadata like:

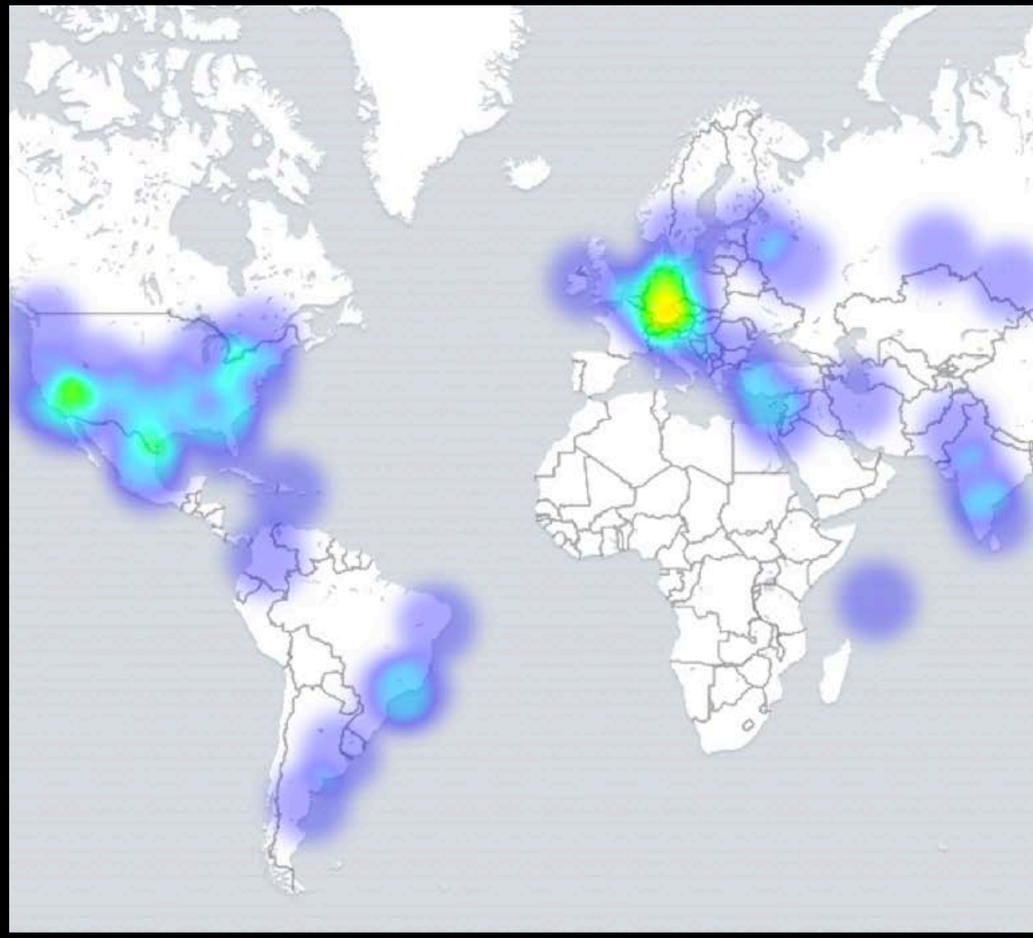
- source
- destination
- packet/byte counts
- timestamps
- type of Service (ToS)
- application ports
- input/output interfaces
- and more

NetFlow – Data Collection

UNIVERSITY OF OXFORD

NetFlow generation at strategic locations: e.g. Internet uplinks, core routers, data centre links

Potential implementations: Cisco kit, Elastic PacketBeat on Linux with PF_RING, or NTOPNG



GeoIP based graph of NetFlow sources

Intrusion Detection isn't Dead

UNIVERSITY OF OXFORD

"IDS as a security technology is going to disappear."

Richard Stiennon, Gartner Research Director, June 2003.

Deployment considerations:

- Inline blocking or passive detection?
- Location, location, location!
  e.g. Internet uplink, Extranet, data centre links, client networks

DNS, the One True King

Logging and analysing DNS traffic can be a challenge, particularly if you host your own DNS services or have a large network.

Potential implementations:

- Log client requests and server responses on your DNS servers (not popular with DNS server administrators).
- Set-up passive DNS collectors like libnmsg or ncap

Get a Handle on Your Data

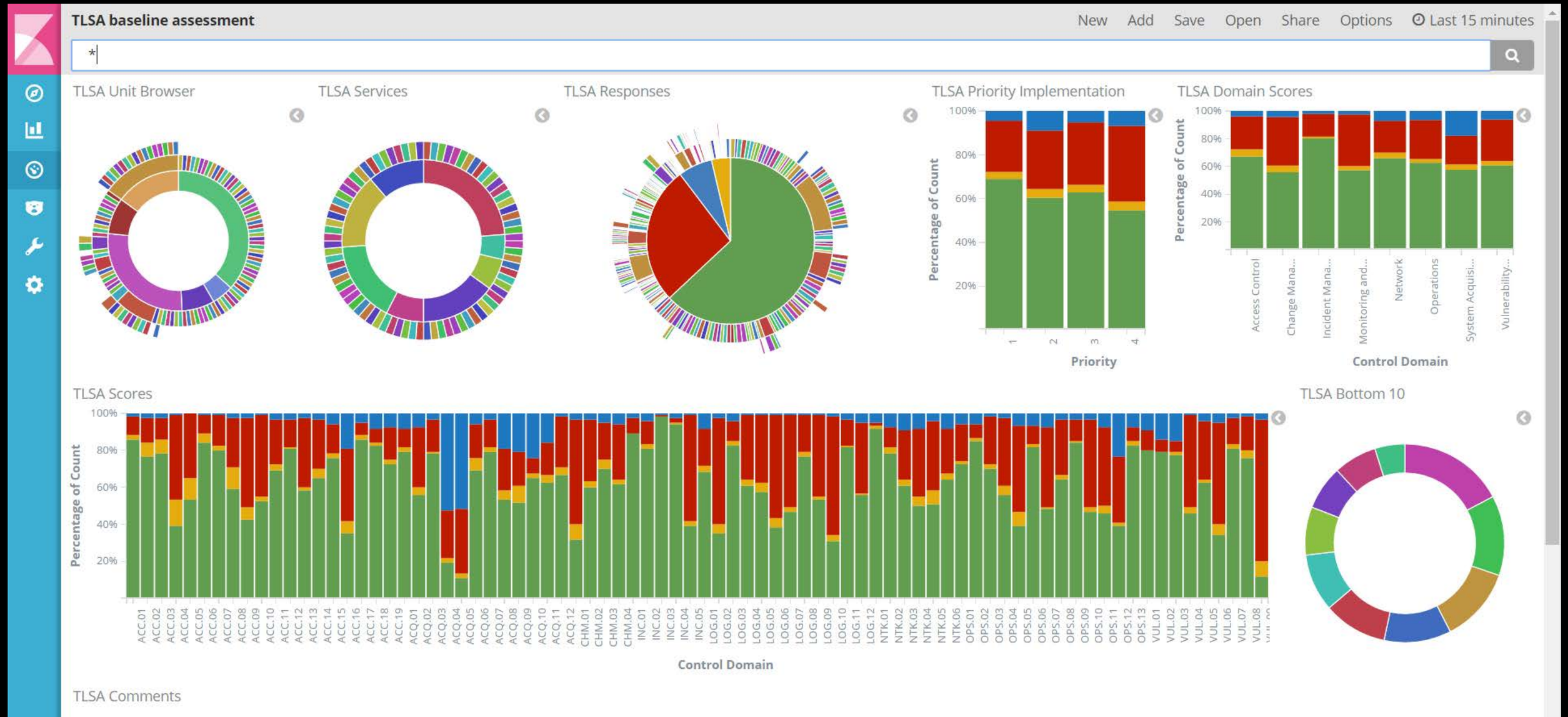
Just collecting all possible logs, events, and alarms does not help making sense out of them! Key lessons learned so far:

- NTP time source, UTC based logging, and ISO 8601 date
- Just the facts – filter and prepare your data
- Normalise your data

  e.g. `2001:420:1101:1::A` vs `2001:420:1101:1:0:0:0:a`
- Maintain consistent keys and curate metadata

Compliance Information

UNIVERSITY OF OXFORD



Compliance Information

Systems report compliance violations to your SIEM solution:

- Endpoint visibility (e.g. osquery, Santa, zentral)
- Server auditing (e.g. OpenSCAP, Lynis)
- Business application auditing (e.g. financial transactions)
- Automated vulnerability Scans (e.g. Nessus)

Nessus Scans Schedules Policies admin

Comprehensive Scan

Share Export Submit for PCI Audit Trail Filter Hosts

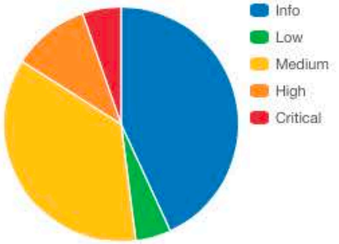
Scans > Hosts 70 Vulnerabilities 225 Remediations 15 Notes 2 Hide Details

Host	Vulnerabilities
172.26.21.251	23 / 219
172.26.21.100	23 / 66 / 8 / 74
172.26.21.103	9 / 72 / 70
172.26.21.220	21 / 7 / 99
172.26.21.106	6 / 47 / 59
172.26.21.148	11 / 81
172.26.21.10	14 / 7 / 70
172.26.21.160	10 / 74
172.26.21.2	7 / 79
172.26.21.18	17 / 6 / 64
172.26.21.159	6 / 22 / 7 / 50
172.26.21.17	14 / 6 / 64
172.26.21.155	6 / 20 / 7 / 52
172.26.21.219	8 / 72
172.26.21.104	6 / 31 / 5 / 37
172.26.21.109	7 / 72
172.26.21.147	7 / 71

Scan Details

Name:	Comprehensive Scan
Folder:	My Scans
Status:	Completed
Policy:	this is the scan to use for PCI
Shared with:	1 user
Scanner:	US Cloud Scanner
Targets:	172.26.21.0/24
Start time:	Wed May 14 12:52:57 2014
End time:	Wed May 14 14:49:40 2014
Elapsed:	2 hours

Vulnerabilities



www.jordan.ox.ac.uk

Results Summary

Critical	High	Medium	Low	Info	Total
0	2	16	2	75	95

Results Details

0/tcp

- 11936 - OS Identification [-/+]
- 12053 - Host Fully Qualified Domain Name (FQDN) Resolution [-/+]
- 19506 - Nessus Scan Information [-/+]
- 25220 - TCP/IP Timestamps Supported [-/+]
- 45590 - Common Platform Enumeration (CPE) [-/+]
- 54615 - Device Type [-/+]
- 66334 - Patch Report [-/+]
- 84239 - Debugging Log Report [-/+]

0/udp

- 10287 - Traceroute Information [-/+]

80/tcp

- 42479 - CGI Generic SQL Injection (2nd pass) [-/+]
- 48926 - CGI Generic 2nd Order SQL Injection Detection (potential) [-/+]
- 39466 - CGI Generic XSS (quick test) [-/+]
- 44136 - CGI Generic Cookie Injection Scripting [-/+]

The Tool Maketh the Team

UNIVERSITY OF OXFORD

SIEM

Security Information and
Event Management

SIRT

Security Incident
Response Tracker

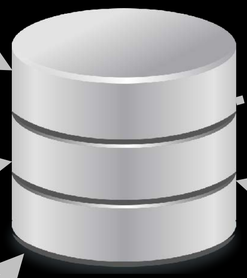
The Tool Maketh the Team

UNIVERSITY OF OXFORD

Logs & Events

Traffic analysis

Compliance



SIEM

Data aggregation
Correlation
Alerting
Retention
Forensic analysis
Reporting

Alerts

Incident data

SIRT

Prioritisation
Workflow
Automation
Threat intelligence
Metadata & Search
Reporting

Incident Reports

Investigation

Countermeasures

The Tool Maketh the Team

UNIVERSITY OF OXFORD

SIEM

SIRT

elastic

https://elastic.co

BEST PRACTICAL™

https://bestpractical.com/rtir/

RTIR: Request Tracker for Incident Response

UNIVERSITY OF OXFORD

Lookup '192.168.1.2' — New ticket in: Incident R — 192.168.1.2

Current Incident: #5

#	Subject	Status	Owner	Last Updated	Told	Created	Due	Priority	Time Left
5	Possible DoS	open	root	1 minute ago		6 weeks ago	2 days	50	

Incidents: 192.168.1.2 — Search

#	Subject	Status	Priority	Actions
2	a problem!	resolved	50	[Merge][Investigate]
5	Possible DoS	open	50	[Investigate]

Investigations: 192.168.1.2 — Search Link

#	Subject	Status	Priority	Actions
10	Possible DoS	open	0	[Link]

Incident Reports: 192.168.1.2 — Search Link

#	Subject	Status	Priority	Actions
1	a problem!	resolved	0	[Link]
4	Possible DoS	resolved	0	[Link]

Blocks: 192.168.1.2 — Search Link Create

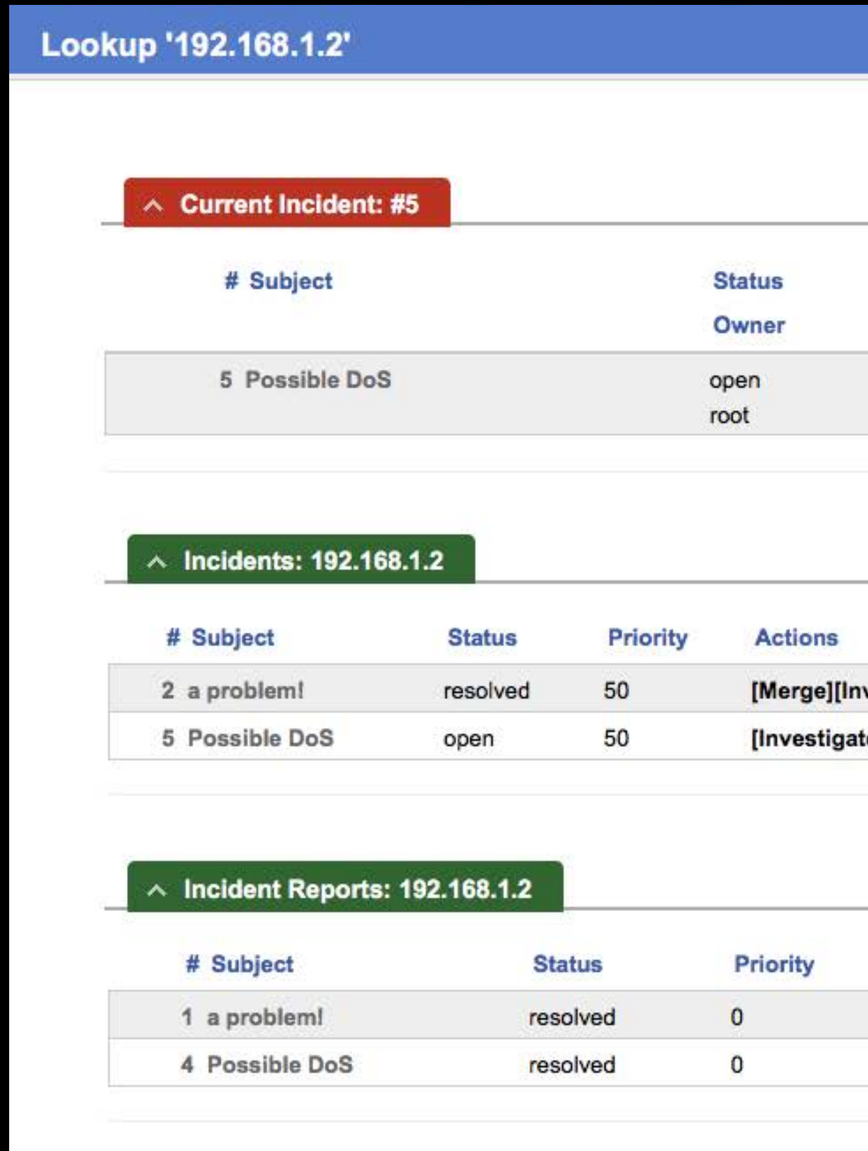
#	Subject	Status	Priority	Actions
3	a problem!	removed	0	[Link]
6	Possible DoS	post incident	0	[Link]

RTIR: Request Tracker for Incident Response

UNIVERSITY OF OXFORD

Incident Tracker shall be also used for

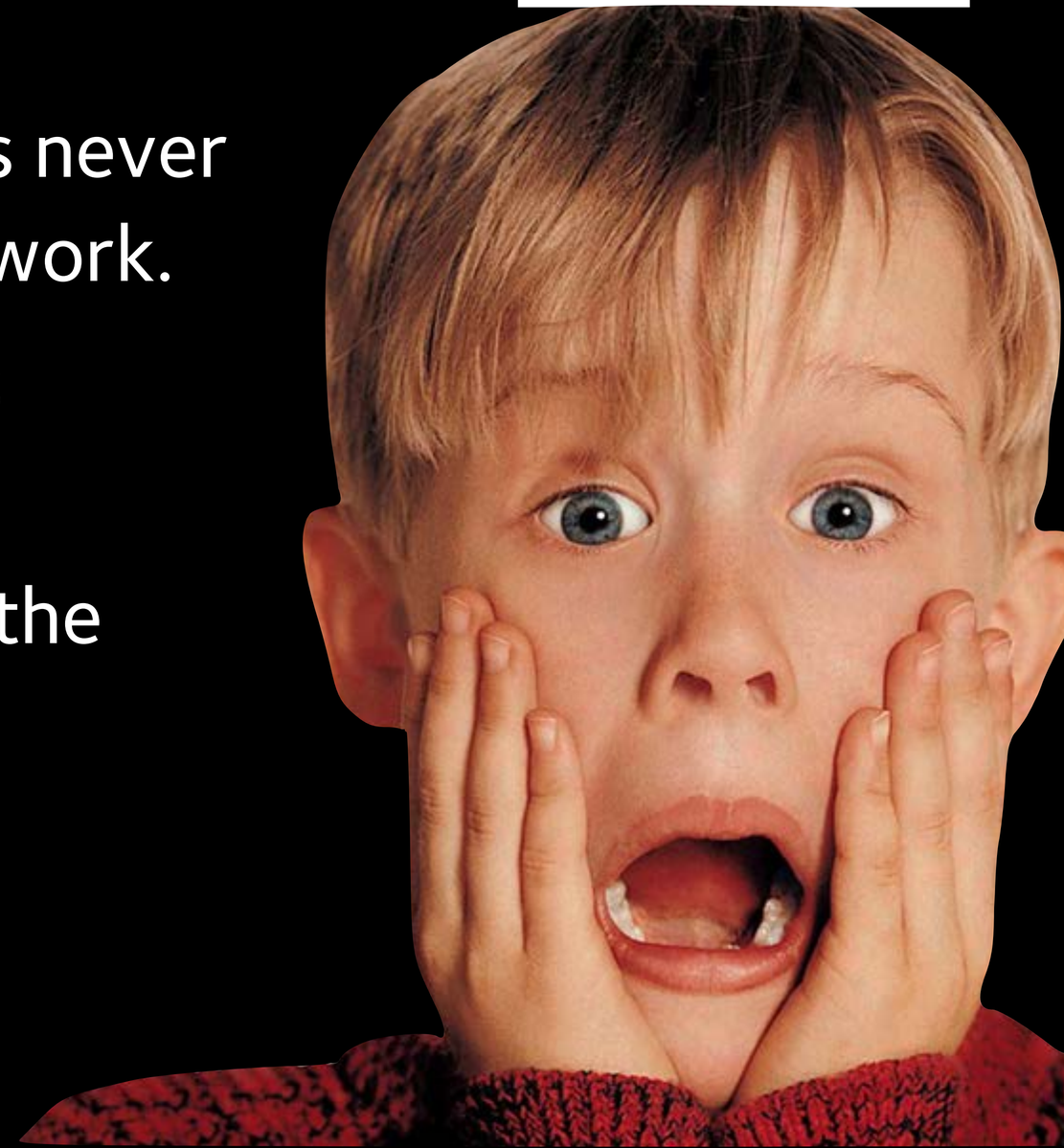
- Phishing
- Third party thread intelligence
- Bulletins
- Vulnerability Scanning
- General advise and guidance
- ...



Yes we are open!

Oxford's network security model has never been based on a trusted internal network.

- The University acts as an ISP to its colleges and departments.
- There is no perimeter firewall for the organisation.
- User services are deployed to the Internet (exceptions apply).



Beyond Corp

"BeyondCorp is an enterprise security model that builds upon 6 years of building zero trust networks at Google"

Principles

- Connecting from a particular network must not determine which services you can access.
- Access to services is granted based on what we know about you and your device.
- All access to services must be authenticated, authorized and encrypted.

SECURITY

BeyondCorp
A New Approach to Enterprise Security

RORY WARD AND BETSY BEYER

Rory Ward is a site reliability engineering manager in Google Ireland. He previously worked in Ireland at Valista, in Silicon Valley at AOL, Netscape, Kiva, and General Magic, and in Los Angeles at Retix. He has a BSc in computer applications from Dublin City University. rorymard@google.com

Betsy Beyer is a technical writer specializing in virtualization software for Google SRE in NYC. She has previously provided documentation for Google Data Center and Hardware Operations teams. Before moving to New York, Betsy was a lecturer in technical writing at Stanford University. She holds degrees from Stanford and Tulane. bbeyer@google.com

Virtually every company today uses firewalls to enforce perimeter security. However, this security model is problematic because, when that perimeter is breached, an attacker has relatively easy access to a company's privileged intranet. As companies adopt mobile and cloud technologies, the perimeter is becoming increasingly difficult to enforce. Google is taking a different approach to network security. We are removing the requirement for a privileged intranet and moving our corporate applications to the Internet.

Since the early days of IT infrastructure, enterprises have used perimeter security to protect and gate access to internal resources. The perimeter security model is often compared to a medieval castle: a fortress with thick walls, surrounded by a moat, with a heavily guarded single point of entry and exit. Anything located outside the wall is considered dangerous, while anything located inside the wall is trusted. Anyone who makes it past the drawbridge has ready access to the resources of the castle.

The perimeter security model works well enough when all employees work exclusively in buildings owned by an enterprise. However, with the advent of a mobile workforce, the surge in the variety of devices used by this workforce, and the growing use of cloud-based services, additional attack vectors have emerged that are stretching the traditional paradigm to the point of redundancy. Key assumptions of this model no longer hold: The perimeter is no longer just the physical location of the enterprise, and what lies inside the perimeter is no longer a blessed and safe place to host personal computing devices and enterprise applications.

While most enterprises assume that the internal network is a safe environment in which to expose corporate applications, Google's experience has proven that this faith is misplaced. Rather, one should assume that an internal network is as fraught with danger as the public Internet and build enterprise applications based upon this assumption.

Google's BeyondCorp initiative is moving to a new model that dispenses with a privileged corporate network. Instead, access depends solely on device and user credentials, regardless of a user's network location—be it an enterprise location, a home network, or a hotel or coffee shop. All access to enterprise resources is fully authenticated, fully authorized, and fully encrypted based upon device state and user credentials. We can enforce fine-grained access to different parts of enterprise resources. As a result, all Google employees can work successfully from any network, and without the need for a traditional VPN connection into the privileged network. The user experience between local and remote access to enterprise resources is effectively identical, apart from potential differences in latency.

The Major Components of BeyondCorp

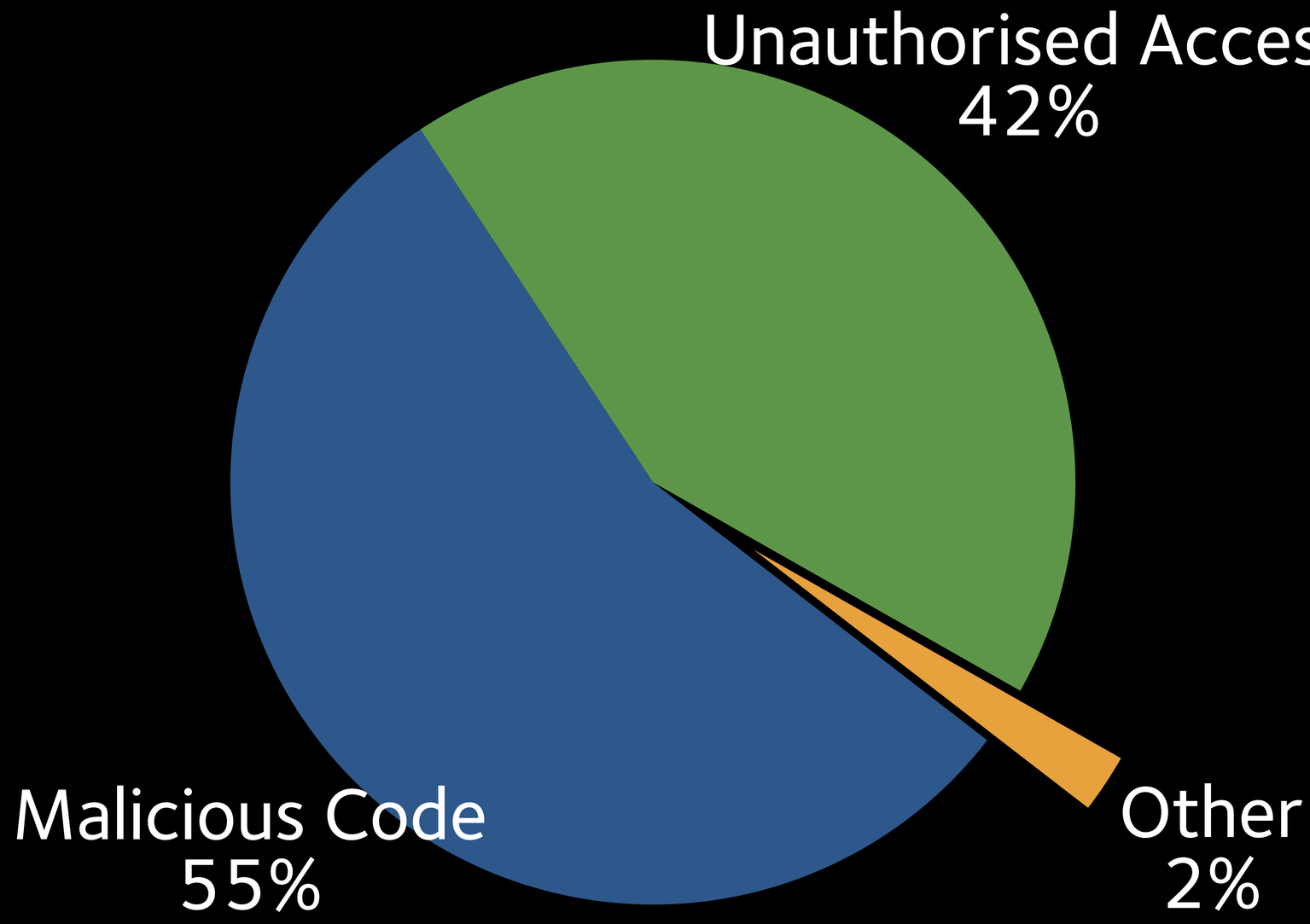
BeyondCorp consists of many cooperating components to ensure that only appropriately authenticated devices and users are authorized to access the requisite enterprise applications. Each component is described below (see Figure 1).

https://research.google.com/pubs/pub43231.html

Most Common Incidents

Incidents 09/10/2016–26/09/2017

UNIVERSITY OF OXFORD



THE TIMES

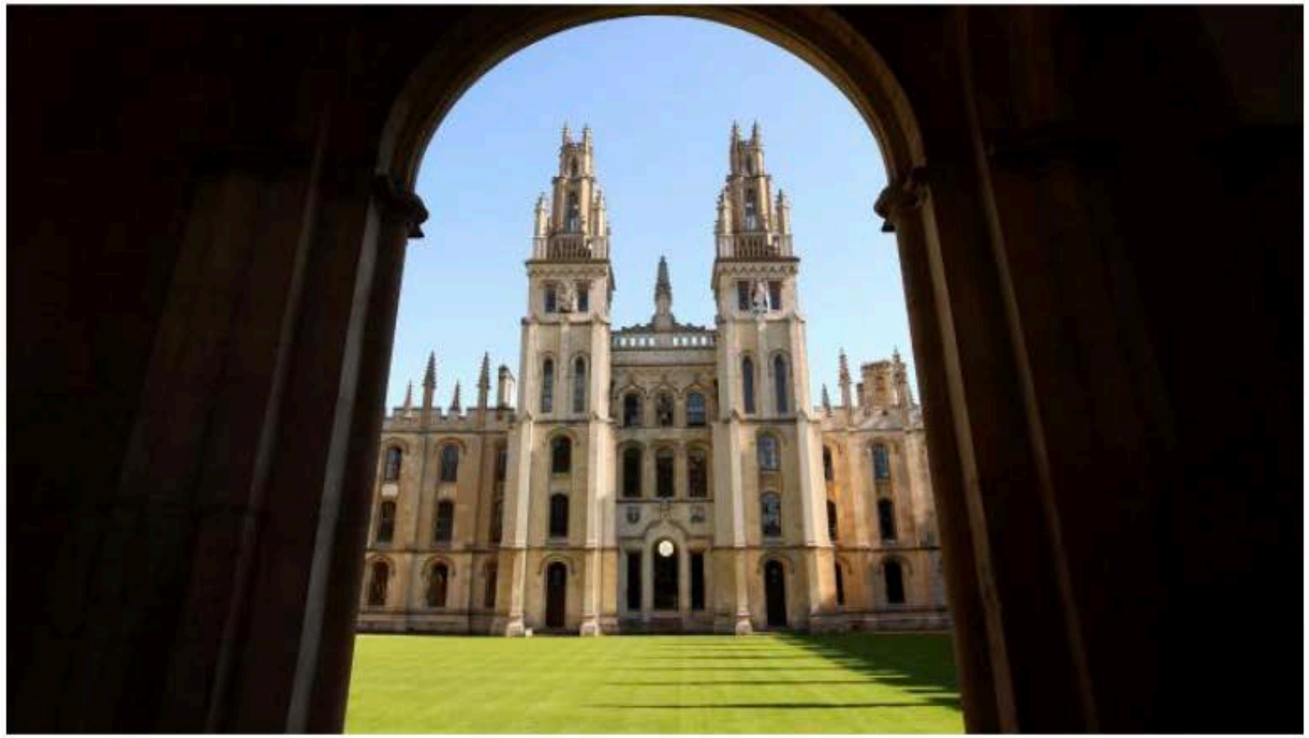
cybergangs

Scientific research targeted by hackers

EXCLUSIVE

Peter Yeung, Rosemary Bennett

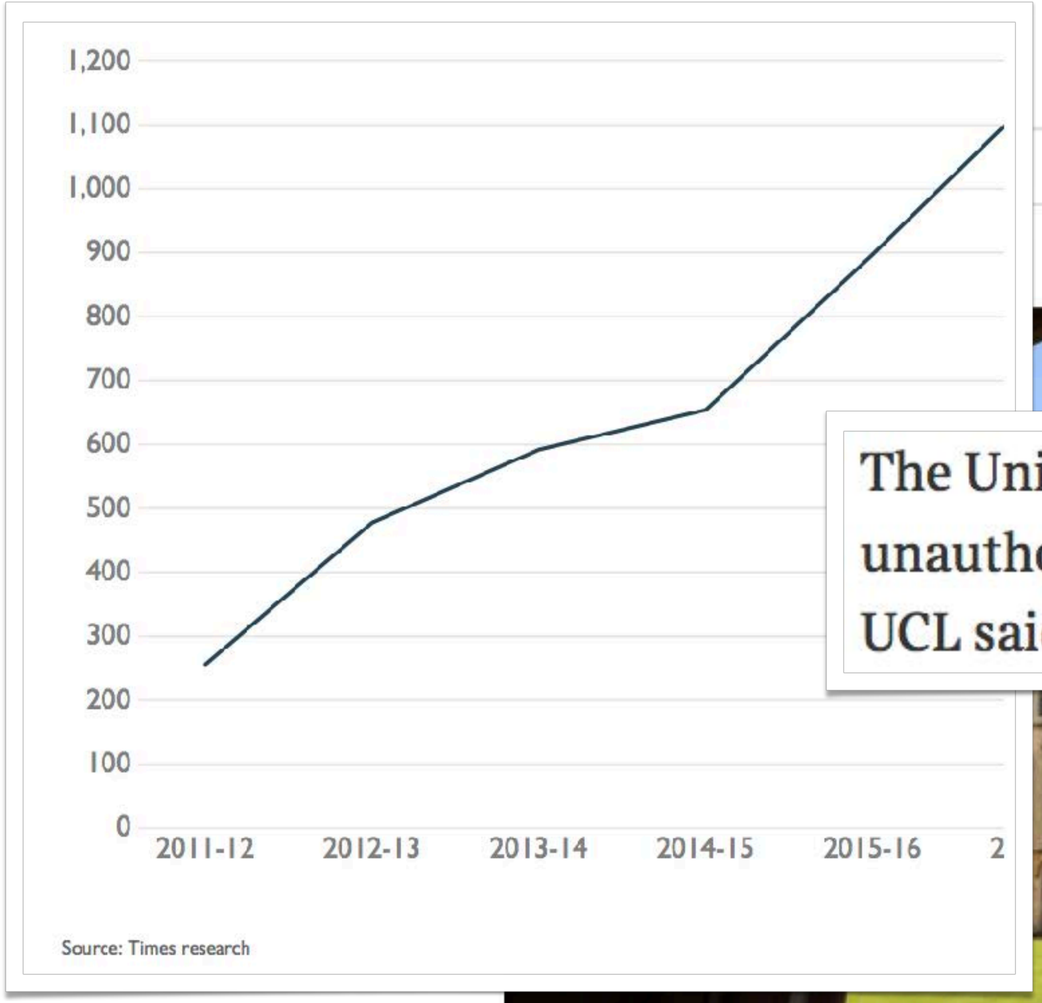
September 5 2017, 12:01am, The Times



THE TIMES

cybergangs

Scientific research targeted by hackers



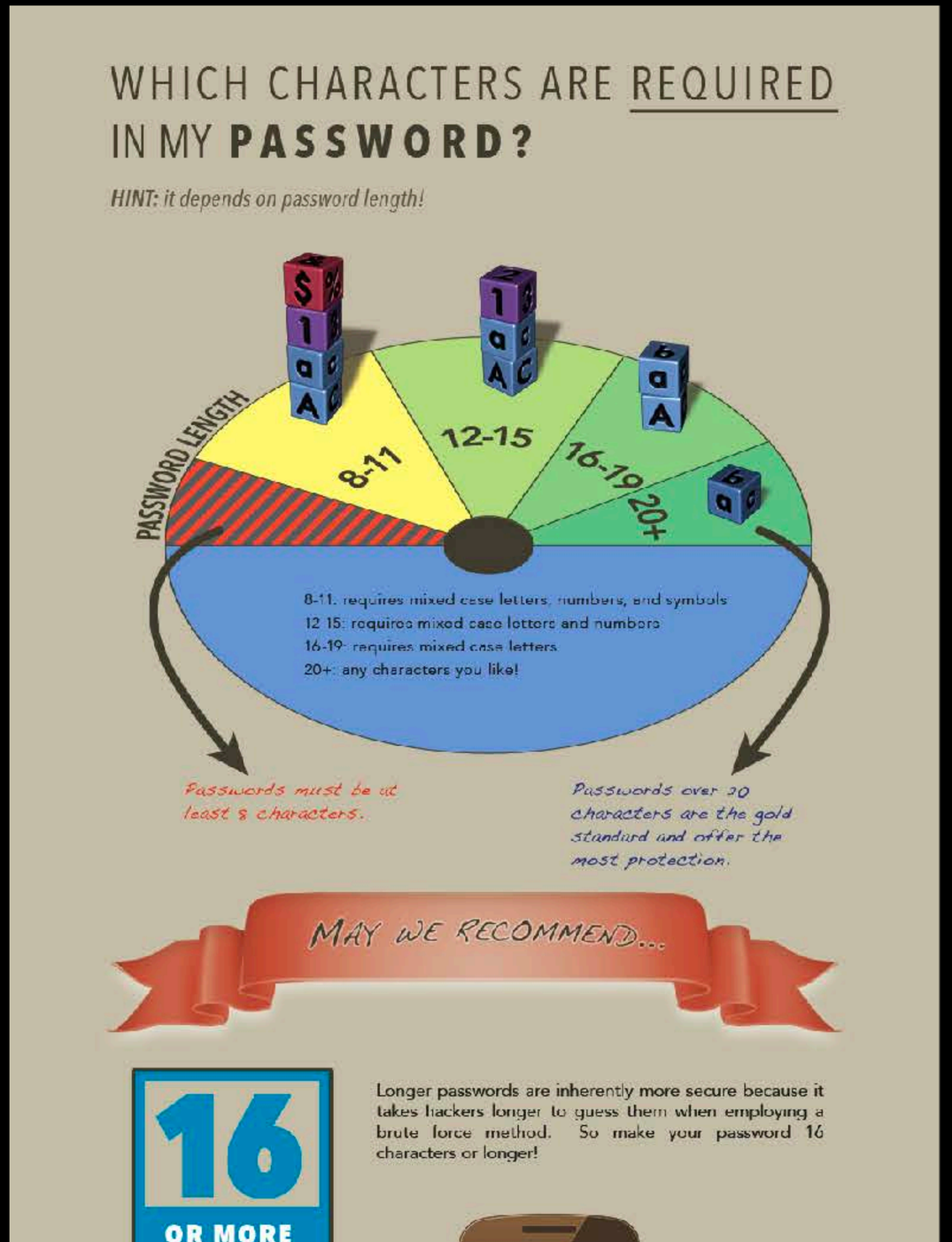
The University of Oxford said there had been 515 cases of unauthorised access to its accounts or machines last year and UCL said that it experienced 57 successful attacks in 2016-17.

Unauthorised Access

We observe the majority of accounts being phished as opposed to hacked.

A good password policy helps.

Ability to lock accounts and audit access is of prime importance.

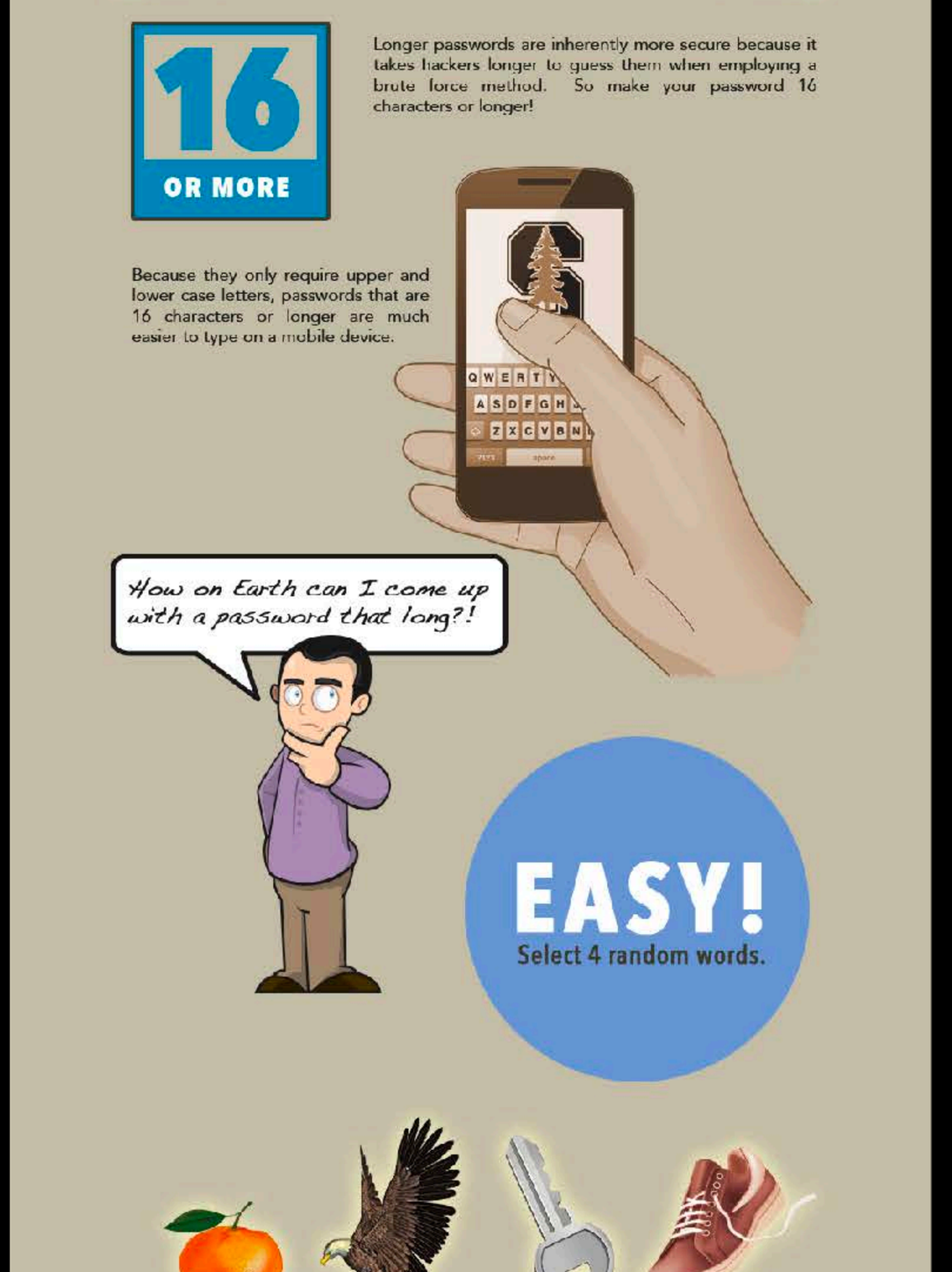


Unauthorised Access

We observe the majority of accounts being phished as opposed to hacked.

A good password policy helps.

Ability to lock accounts and audit access is of prime importance.



Unauthorised Access

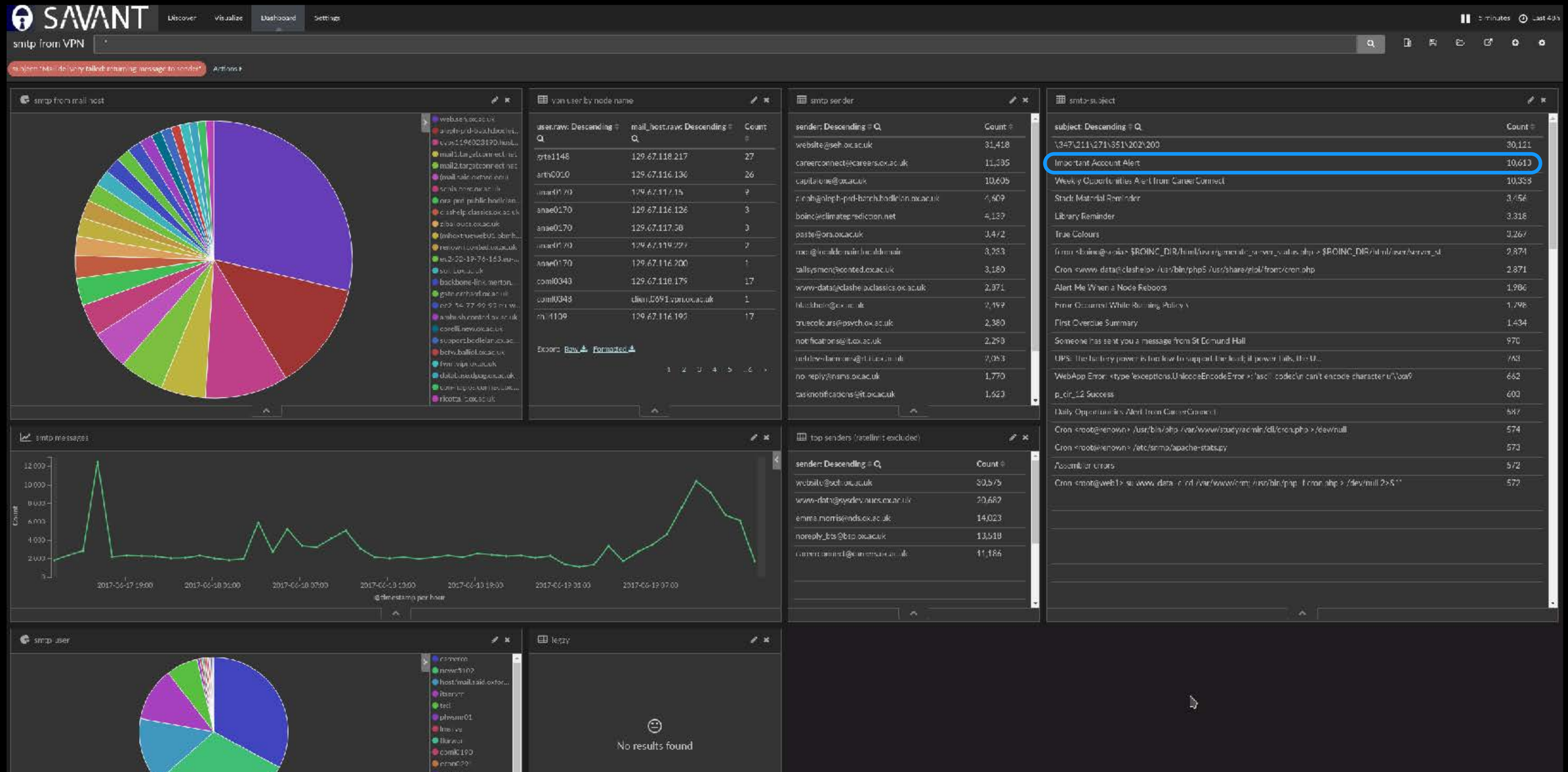
We observe the majority of accounts being phished as opposed to hacked.

A good password policy helps.

Ability to lock accounts and audit access is of prime importance.

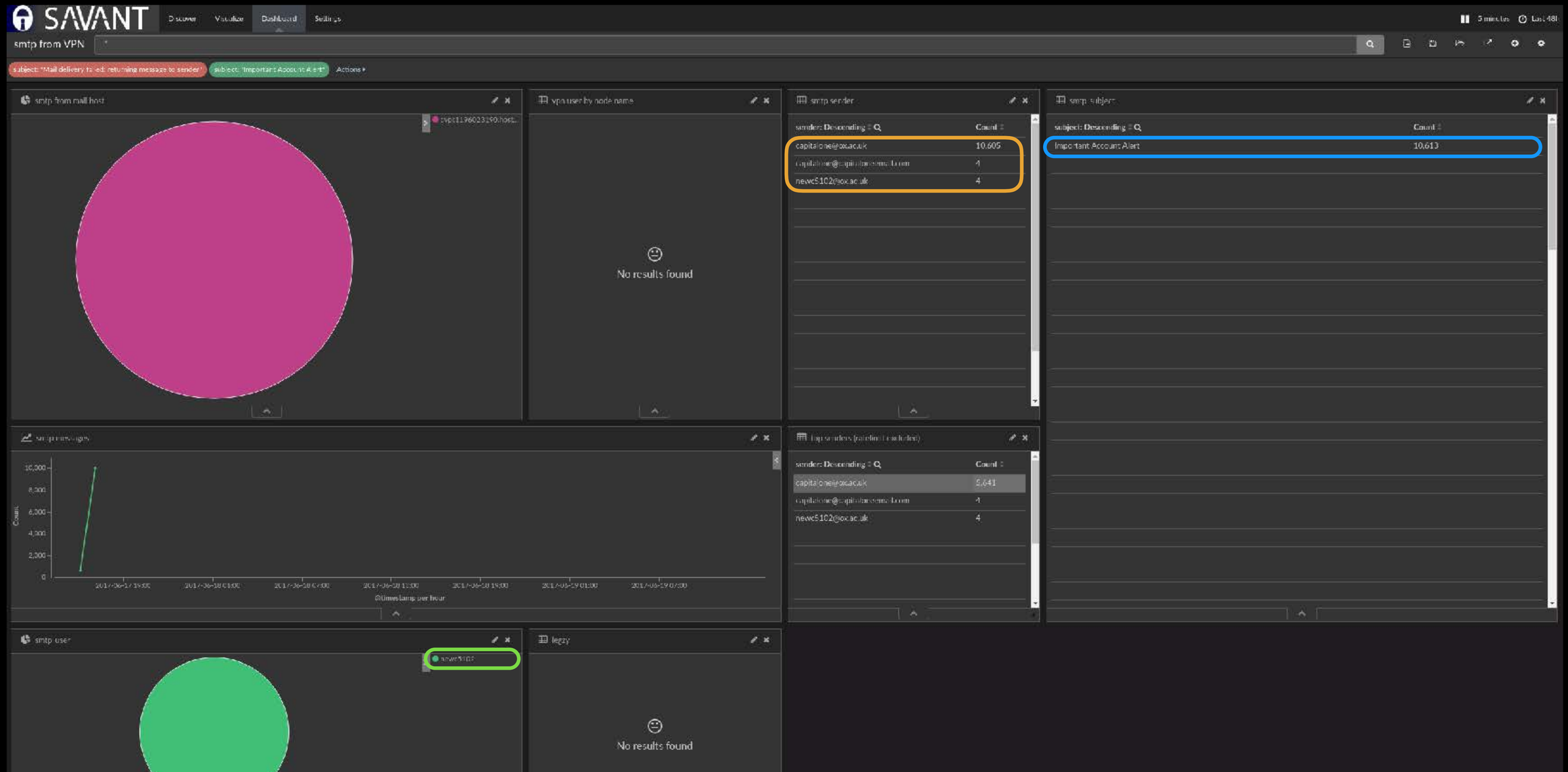
Example: Spammer

UNIVERSITY OF OXFORD



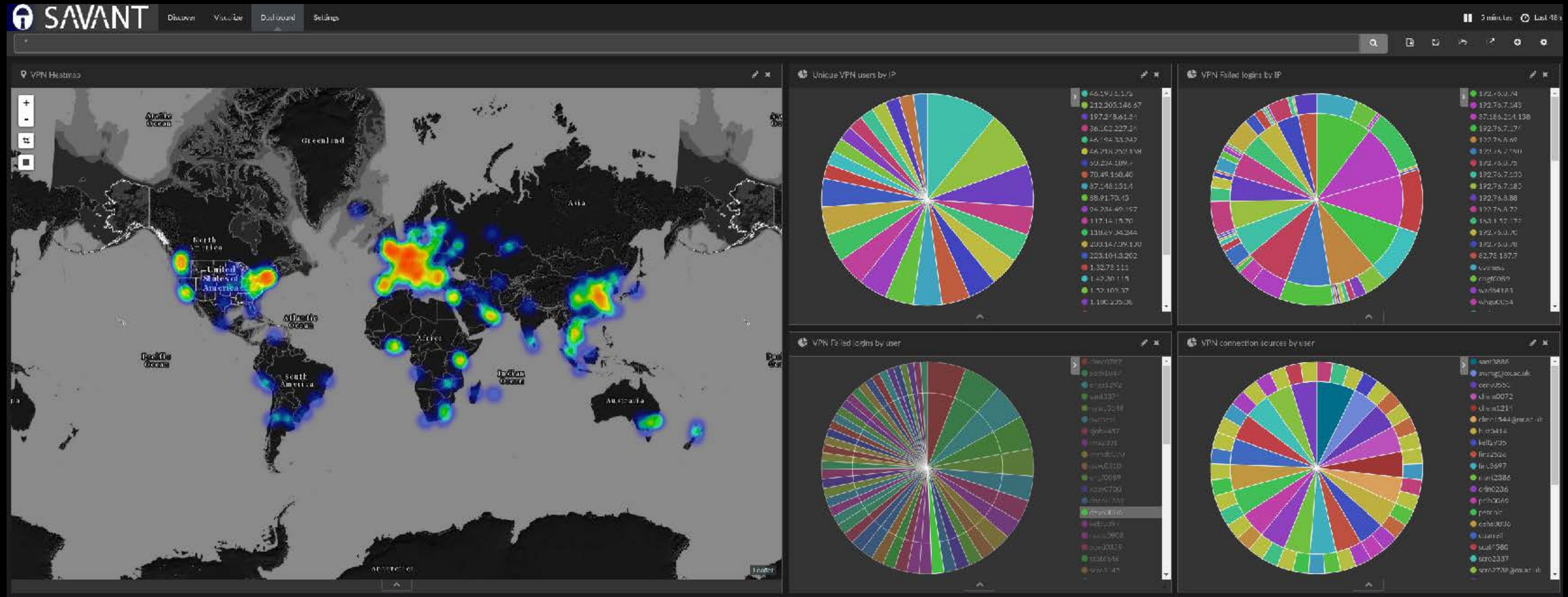
Example: Spammer

UNIVERSITY OF OXFORD

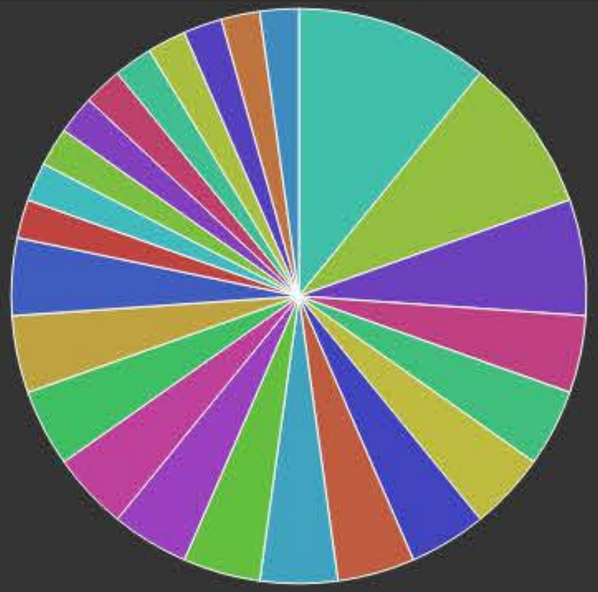


Example: VPN Abuse

UNIVERSITY OF OXFORD

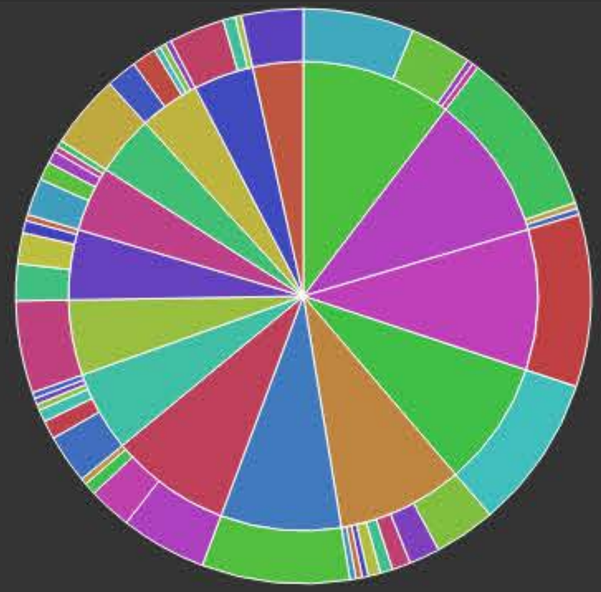


Unique VPN users by IP



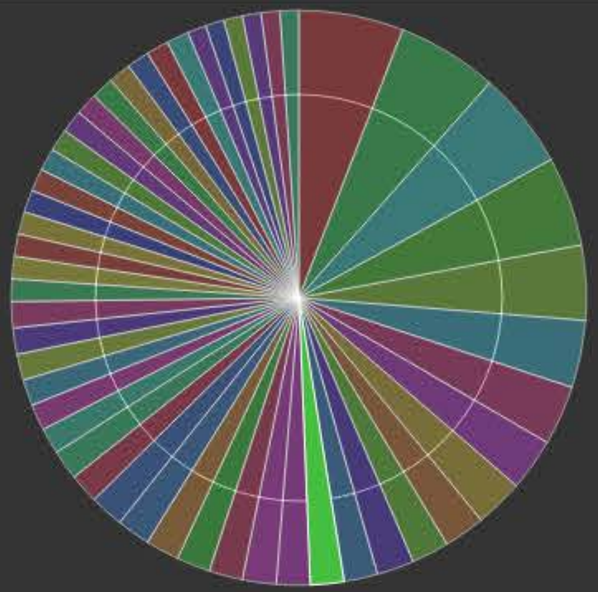
46.193.1.172
212.205.146.67
197.248.61.34
36.102.227.24
46.194.33.242
46.218.252.158
50.234.189.7
78.49.168.40
87.148.151.4
88.91.70.45
94.234.49.197
117.14.15.70
118.69.34.244
203.147.39.130
223.104.3.202
1.32.73.111
1.42.30.115
1.52.109.37
1.180.235.38

VPN Failed logins by IP



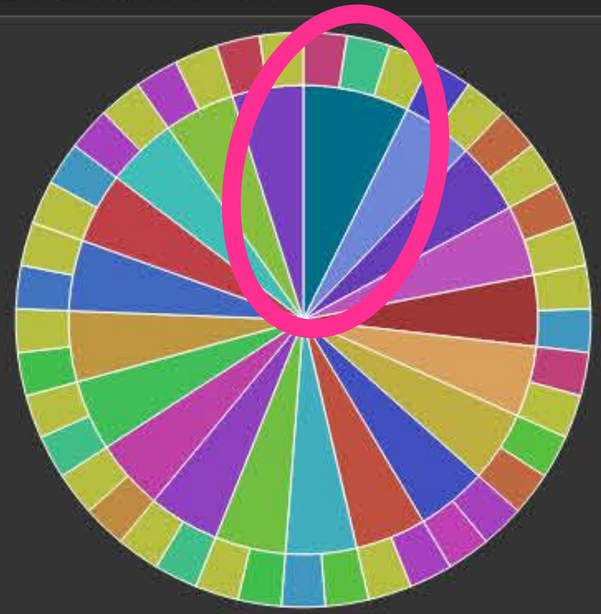
192.76.8.74
192.76.7.143
37.186.214.138
192.76.7.174
192.76.8.69
192.76.7.190
192.76.8.75
192.76.7.133
192.76.7.185
192.76.8.88
192.76.8.72
163.1.57.172
192.76.8.70
192.76.8.78
82.73.187.7
oveness
engf0089
wadh4183
whgu0054

VPN Failed logins by user



clme0787
path1047
engs1292
sant3374
newc3148
oveness
sjoh4457
lina2831
immd0370
psyc0310
engf0089
xpsy0700
chem1239
devo0086
kebl3397
manc0908
paed0359
scat6646
scro3145

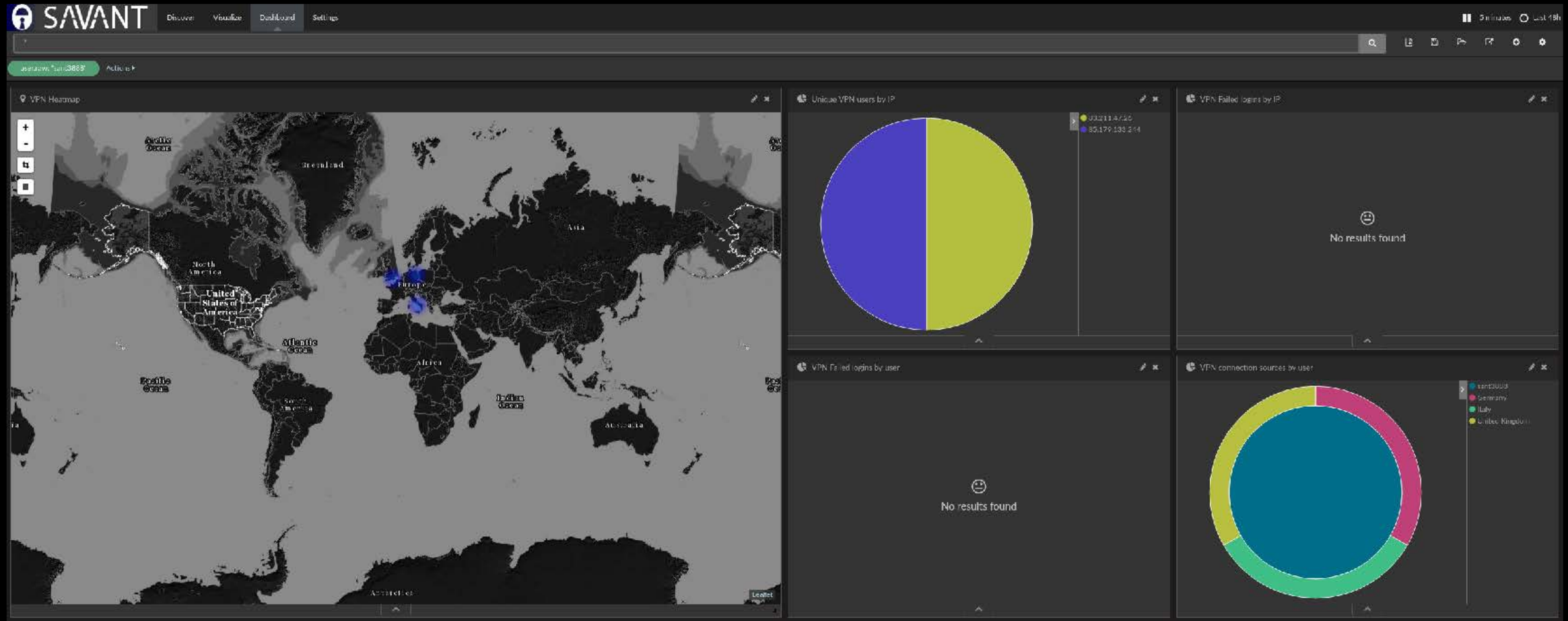
VPN connection sources by user



sant3888
awmg@ox.ac.uk
cenv0553
chem0072
chem1214
clme1544@ox.ac.uk
hist0414
kell2935
lina2526
linc3697
mert2386
orin0236
pclb0069
petrinic
qehs0836
quarrell
scat4580
scro2337
scro2738@ox.ac.uk

Example: VPN Abuse *(continued)*

UNIVERSITY OF OXFORD



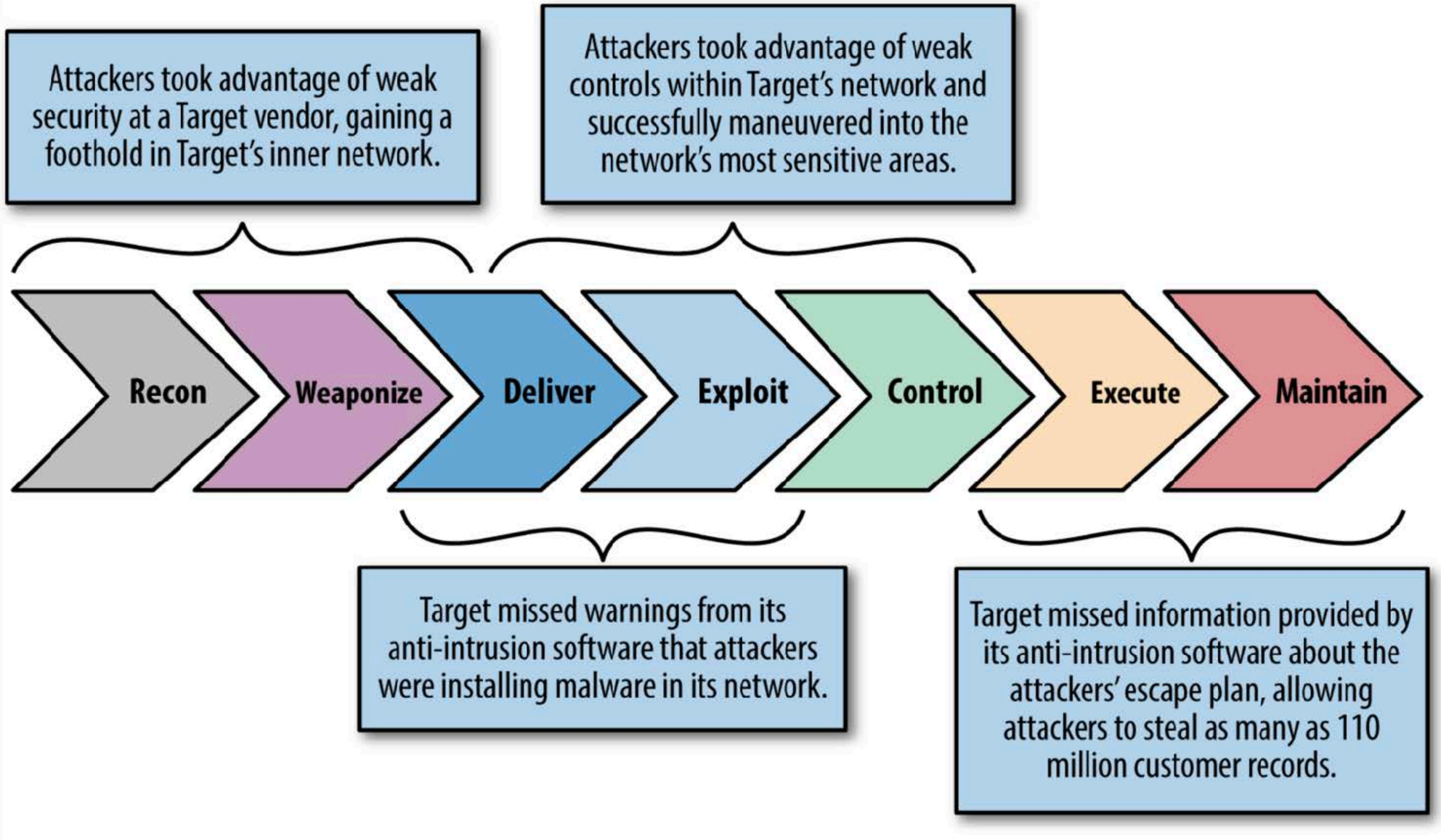
Strategies for Phishing?

User education on phishing: continuous awareness campaigns, training, internal phishing exercises.

Response Policy Zone (RPZ) to subvert phishing sites to a sinkhole.

Email security products, e.g. Mimecast, Advanced Email Threat Protection, Hosted Email Security, …

Malicious Code: The Kill Chain



Measure Up

There are several ways to measure a team's detection efficiency with a few simple metrics such as the following:

- How long it takes to detect an incident after it occurred?
- How long it takes to contain an incident after its detection?
- How long it takes to analyse an alert or solve an incident?
- How many infections are blocked or avoided?
- How well are playbook reports performing?

Further Reading

Jeff Bollinger, Brandon Enright, and Matthew Valites: Crafting the InfoSec Playbook

O'Reilly; 1st edition (6 May 2015)
http://oreilly.com/catalog/errata.csp?isbn=9781491949405

Aaron Bradley: OS X Incident Response

Syngress/Elsevier; 1st edition (6 May 2016)
https://www.elsevier.com/books/os-x-incident-response/bradley/978-0-12-804456-8

Thank You!


https://github.com/mjung/publications

Marko Jung

Galactic Viceroy of Research Excellence


m@mju.ng


@mjung


fb.com/markohjung